

FILED IN CLERK'S OFFICE

U.S.D.C. Atlanta

MAY 25 2016

JAMES N. HATTEN, Clerk
By: *[Signature]* Deputy Clerk

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,

v.

KEVIN M. SULLIVAN,

Defendant.

CRIMINAL ACTION

NO. 1:15-CR-290-MHC-CMS

**ORDER AND REPORT AND RECOMMENDATION OF
UNITED STATES MAGISTRATE JUDGE**

On August 5, 2015, a Grand Jury sitting in the Northern District of Georgia returned a two-count indictment against Defendant Kevin M. Sullivan for charges relating to the receipt and possession of the visual depiction of a minor engaging in sexually explicit conduct. (Doc. 11). This case is before the Court on Defendant's Motion to Suppress and Supplemental Motion to Suppress (Docs. 26, 33) in which he argues that the warrant used by law enforcement to search his office at Emory University did not satisfy the particularity requirement of the Fourth Amendment.¹

¹ Also pending is Defendant's Motion for Bill of Particulars and for Further Rule 16 Discovery and Brady Information. (Doc. 27). Defense counsel has informed me that this motion has been resolved, and accordingly it will be denied as moot.

As discussed below, I **RECOMMEND** that Defendant's motions to suppress be **DENIED**.

I. FACTUAL BACKGROUND

On February 22, 2016, I conducted an evidentiary hearing on Defendant's Motion to Suppress. (Doc. 38, Transcript ["Tr."]). At the hearing, the Government presented the testimony of Sara Thomas, a special agent with the Georgia Bureau of Investigation ("GBI") who also serves as a task force agent with Homeland Security Investigations ("HSI"). (Id. at 11). The Government also called Matthew Heath, a digital forensic investigator with the GBI child exploitation and computer crimes unit. (Id. at 61-62).

Agent Thomas testified that the investigation leading to Defendant's indictment arose out of a criminal investigation in Switzerland in which a computer server was seized, leading investigators to a child pornography website and a long list of Internet Protocol ("IP") addresses. (Tr. at 12-13). Agent Thomas explained that an IP address is assigned by the internet service provider and can show the location where a certain device is at the time it accesses the Internet. (Id. at 13). The IP address stays within a location, such as in a building. (Id. at 14). Swiss law enforcement officers used the list of IP addresses to determine the locations where child pornography was being uploaded and downloaded. (Id. at

13). The Swiss officials sent information regarding the IP addresses in the United States on the list to the HSI Cyber Crimes Center in Washington, D.C. (Id.).

Ultimately, the investigation into one IP address on the list led U.S. law enforcement to Emory University in Atlanta, Georgia. (Tr. at 14). At that time, federal agents contacted Emory University, which cooperated with the investigation. (Id.). With Emory's assistance, the investigators determined that the public wireless network in Emory's Claudia Nance Rollins Building (the "Rollins Building") was being used to facilitate the downloading of the child pornography. (Id. at 15-16). They were also able to identify the specific Media Access Control address ("MAC address") of the device that had downloaded child pornography as well as the name associated with that device: "Kev-HP." (Id. at 14-15). Agent Thomas testified that a MAC address is unique to each particular device. (Id. at 14). If, for example, someone accesses the Internet on her phone in multiple locations, the IP address will change based on the different places where she accesses the Internet, but the phone's MAC address will not change. (Id. at 15). At this point in the investigation, law enforcement knew that someone was using the public wireless internet within the Rollins Building to access child pornography, and they knew the MAC address for the device was "Kev-HP"; they did not know,

however, where the device was located within the building or who was using it. (Id. at 16).

After receiving this information, Agent Thomas spoke with other agents who informed her of the existence of a device called a “sniffer” that could be used in an area to limit the search and to help identify the location of a certain device with a particular MAC address. (Tr. at 16). Agent Thomas testified that, “Just like a dog sniffs out for a certain smell, this device sniffs out for certain packets being transmitted from a device to the wireless network.” (Id. at 17-18). Agent Thomas testified that unlike a “triggerfish” or similar system that forces a signal or mimics a cell phone tower, the sniffer does not interfere with, or interrupt the flow of, electronic communications. (Id. at 18-19). For a sniffer to work, the device it is looking for must be turned on. (Id. at 19).

On June 5, 2015, Agent Thomas obtained a search warrant from the Superior Court of DeKalb County, Georgia. (Tr. at 16). The application for the warrant contained a lengthy, detailed sworn statement by Agent Thomas that summarized the evidence that her investigation had revealed. (Doc. 33-1, Search Warrant, at 4-16). It set forth the history of the investigation and the evidence that led law enforcement to the Rollins Building. (Id. at 5-9). The affidavit described the plan to use a sniffer to “identify the wireless device associated with the suspect MAC

address, '68:a3:c4:e2:6a:7e', that has been identified in this investigation." (Id. at 9, Tr. at 34). The actual warrant, however, did not mention the sniffer; rather, it authorized the search of the entire building, without limitation and without reference to the sniffer. (Doc. 33-1 at 1-2). The location listed on the warrant is "Emory University's Claudia Nance Rollins Building, School of Public Health, 401 Rollins Way in Atlanta, DeKalb County, Georgia. See attached picture. . . ." (Id. at 1). The picture attached was an outside photograph of the entire building. (Tr. at 30-31). The warrant instructed agents to search for a number of items, including a "wireless device containing the Medial [sic] Access Control (MAC) address '68:a3:c4:e2:6a:7e.'" (Doc. 33-1 at 1).

Four days later, on June 9, 2015, Agent Thomas and her team went to Emory University with the intention of executing the search warrant. (Tr. at 29). When they arrived, however, they learned that the device was not being used to access the network at that time. (Id. at 21, 22). While at Emory, they met with an Emory IT specialist, Derek Spransy, who provided additional information. (Id. at 20). Mr. Spransy confirmed that the name of the suspect device was "Kev-HP." Mr. Spransy stated that he had located three people named "Kevin" who worked at Emory, one of whom—Defendant Kevin Sullivan—worked in the Rollins Building, in Room 3051. (Id. at 20-21, 39). He stated that Sullivan was not in the

office that day and was on leave for the entire week. (Id. at 21). During the June 9 meeting, Mr. Spransy also reported that he had determined that the device in question had frequently visited certain wireless access points within the building, one directly below Sullivan's office (Room 2051), and one directly next to Sullivan's office (Room 3049). (Id. at 21, 51). Later that week, Mr. Spransy informed the agents that the suspect device had not accessed Emory's wireless network that entire week. (Id. at 21).

When asked on cross-examination about why law enforcement did not obtain a more particularized warrant after this additional information was acquired, Agent Thomas testified that despite the new information from Mr. Spransy, her team still did not know whether Defendant Sullivan was involved, and she did not consider him to be a suspect at that time. (Tr. at 39, 51-52). She pointed out that the area around the identified access points was an "open area" where both students and professors could be (implying that the operator of the device was not necessarily located in a particular faculty office), and that sometimes people buy computers and other devices from other people (implying that the computer name "Kev-HP" could be operated by anyone, not necessarily a person named Kevin). (Id. at 40; Doc. 33-1 at 8).

Six days later, on June 15, 2015, Agent Thomas received a call from Emory University indicating that the suspect device was utilizing the network that day, at which point Agent Thomas assembled her team, went to the Rollins Building, and executed the warrant. (Tr. at 22-23, 41). Two sniffers were used, one by a GBI investigator and the other by a detective from the DeKalb County Police Department. (Id. at 23). The sniffer operators split up, going to the second and fourth floors in an attempt to locate the device, and both reported no readings on their respective floors. (Id. at 24). They then moved to the third floor where they obtained readings near Defendant's office. (Id. at 24-25). Although there were multiple offices on the third floor, the strongest readings were coming from Defendant's office. (Id. at 26).

Defendant's office has clouded glass windows, the door was locked, and there was a yellow sticky note on the door that read, "Please do not unlock door." (Tr. at 26). Agent Thomas knocked on the door, and then she heard "a bang and a click" and a male voice asking who was knocking. (Id.). At that point, the sniffer lost the signal. (Id. at 53, 59). Agent Thomas said, "Mr. Sullivan, I need to speak with you." (Id. at 27). Defendant came to the door and opened it slightly. Agent Thomas identified herself as a special agent with the GBI, informed him that they were executing a search warrant, and asked if she could speak with him. (Id.).

Defendant asked if he was under arrest, and Agent Thomas said that he was not under arrest but that she wanted to speak with him. (Id.). Defendant exited his office and went with Agent Thomas to a room on the opposite side of the building. (Id. at 28). The interview did not last long. After Agent Thomas advised Defendant of his Miranda rights, he asked to speak with an attorney. (Id.).

Meanwhile, other members of the investigation team conducted a search of Defendant's office, where they located the computer with the MAC address that they were looking for. (Tr. at 28). A forensic preview of an external hard drive connected to the laptop with the suspect MAC address revealed child pornography. (Id. at 53-54). The agents seized two laptop computers (one of which was the suspect device), a desktop computer, a cell phone, "a few" flash drives, and the external hard drive. (Id. at 28-29).

On cross-examination, defense counsel asked whether the agents thought about obtaining a new, more specific warrant before knocking on Defendant's door. (Tr. at 44). Agent Thomas stated that before she got the warrant, she had sought advice from attorneys at Homeland Security and Emory about whether the warrant would be sufficient and had been advised that the warrant would be sufficient for her purposes. (Id. at 44-45, 59-61). Agent Thomas also testified that the warrant could not be narrowed in terms of location because, given the mobile

nature of the suspect device, they did not know where they would find it at any given time; it could have been in a student's backpack, for example, or in a faculty member's office. (Id. at 47-48).

II. ANALYSIS

The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. Thus, the Fourth Amendment requires that a warrant particularly describe both (1) the place to be searched and (2) the persons or things to be seized. Id.; United States v. Travers, 233 F.3d 1327, 1329 (11th Cir. 2000). The Fourth Amendment's particularity requirement safeguards the individual against “the wide-ranging exploratory searches the Framers [of the Constitution] intended to prohibit.” Maryland v. Garrison, 480 U.S. 79, 84 (1987).

A search based on a warrant that fails to sufficiently particularize the place to be searched or the things to be seized is unconstitutional. U.S. Const. amend. IV. To deter such warrants and searches, any evidence so seized must be excluded from the trial of the defendant. Stone v. Powell, 428 U.S. 465, 492 (1976) (“Evidence obtained by police officers in violation of the Fourth Amendment is excluded at trial in the hope that the frequency of future violations will decrease.”).

Defendant argues that the warrant was not sufficiently particularized with respect to either the place to be searched or the things to be seized. In response, the Government argues, among other things, that (1) the warrant was sufficiently particularized, especially when viewed in combination with the supporting affidavit and the knowledge of the agents on site when the warrant was executed and (2) even if the warrant was invalid for some reason, the evidence still should not be excluded because the good faith exception to the exclusionary rule applies.²

² The Government also makes the alternative argument that exigent circumstances existed to justify a warrantless search. The test used to determine whether exigent circumstances exist is an objective one: “[t]he appropriate inquiry is whether the facts . . . would lead a reasonable, experienced agent to believe that evidence might be destroyed before a warrant could be secured.” United States v. Tobin, 923 F.2d 1506, 1510 (11th Cir. 1991) (en banc) (internal quotation marks omitted). The Government argues that Defendant could have realized that he was about to be arrested and then could have destroyed the evidence before agents returned with a search warrant. The record does not support this argument. There is no testimony that Defendant knew he was being investigated until the agents knocked on his office door. The testimony was that it was not until *after* Agent Thomas knocked on the door that she heard “a bang and a click,” which she believed to be the sound of a laptop closing, at which point the sniffer lost the signal. (Tr. at 53, 59). Law enforcement cannot create the exigent circumstances and then rely on those circumstances to perform a warrantless search. See United States v. Coles, 437 F. 3d 361, 370 (3d. Cir. 2006). Moreover, after Defendant opened the door and was removed from his office, the agents had control of his office without any concern about destruction of evidence. (Tr. at 90).

A. Particularity

Defendant argues that the warrant in this case is not sufficiently particularized, both with respect to the place to be searched and the things to be seized.

1. The place to be searched

The warrant provides the following description of the place to be searched: “Emory University’s Claudia Nance Rollins Building, School of Public Health, 401 Rollins Way in Atlanta, DeKalb County, Georgia. See attached picture [of the outside of the Rollins Building].” (Doc. 33-1 at 1).

A warrant sufficiently particularizes the place to be searched if the executing officers can “with reasonable effort ascertain and identify the place intended.” Steele v. United States, 267 U.S. 498, 503 (1925); United States v. Burke, 784 F.2d 1090, 1092 (11th Cir. 1986) (holding that a warrant must describe the place to be searched with sufficient particularity “to direct the searcher, to confine his examination to the place described, and to advise those being searched of his authority”).

In his briefs in support of his motion to suppress, Defendant first argues that by identifying the entire Rollins Building as the place to be searched, the warrant fails to identify the place to be searched with sufficient particularity, noting that the

warrant purports to authorize agents to search anywhere in the building. (Docs. 33, 39, 42). Defendant argues that “the agents were given free reign [sic] to search virtually any one and any thing in the largest building on campus and the court had to rely on the agents to govern themselves.” (Doc. 39 at 2). The Government responds that the warrant was as specific as it could have been, given the circumstances and nature of the investigation. (Doc. 40 at 7).

Defendant argues that the warrant could have been more narrowly tailored based on the information the agents acquired from Mr. Spransy, but the record does not support this position. Agent Thomas testified that when the agents applied for the warrant, Defendant was not a confirmed suspect. (Tr. at 40, 51, 52). And, even if Defendant were a suspect, the record does not reflect that the search could have been more limited because it was not known whether the device was located in an office, or in a backpack, or at any other place within the building. (Id. at 47-48). Even though certain floors in the building may have been of more interest to the investigators as they began their search, the agents could not rule out any portion of the building until they actually used the sniffer.

The Eleventh Circuit approved a similar warrant in United States v. Rousseau, 628 F. App’x 1022 (11th Cir. 2015). Like the present case, Rousseau involved someone accessing an open wireless network at a workplace to download

child pornography. Id. at 1024. The wireless network in Rousseau covered the front portion of a fire station where emergency vehicles were housed. The warrant described the property to be searched very broadly, as, among other things, any computers, data storage devices, and cellular telephones found in the fire station. Id. at 1026. In rejecting the defendant's contention that the warrant was not sufficiently particular in terms of the location to be searched, the Eleventh Circuit stated:

To the extent the descriptions did not identify a specific location within the Station or specific item (such as a particular computer or cell phone), they were as specific as the circumstances and nature of the activity being investigated would permit. The agents were investigating the downloading and sharing of child pornography using an IP address registered to the Station and an open wireless network accessible inside the Station. The investigators did not know which or how many Station employees might be involved in the activity, much less which computers or electronic storage devices in the Station were being used. The warrant made clear that a search of the computers required the seizure of "most or all computer items" to perform the search thoroughly, and that "on-site evidentiary previews" would be conducted to minimize the burden on individuals and devices that were not involved in the illegal activity. The warrant also only authorized the seizure of items that were "[e]vidence of possession, receipt, and distribution of child pornography."

Id. at 1027. In some respects, the warrant in Rousseau, which authorized a search of every computer and cell phone in the fire station, was broader than the warrant for the Rollins Building in this case. The fact that the Eleventh Circuit approved of the warrant in Rousseau, therefore, weighs in favor of finding that the warrant's

description of the entire Rollins Building as the place to be searched was sufficiently particular to satisfy the Fourth Amendment.

Defendant's concerns about the risk that law enforcement would perform a general search of everyone and everything in the Rollins Building pursuant to the warrant are allayed by the fact that the affidavit describes how a sniffer works and indicated that the agents intended to use the sniffer to perform a focused, targeted search to locate the suspect device. The Eleventh Circuit has held that under similar circumstances, a court can consider the content of a supporting affidavit when ruling on a Fourth Amendment challenge to a warrant. See United States v. Martinelli, 454 F.3d 1300, 1308 (11th Cir. 2006) (holding that a warrant was not overbroad due to failure to identify the crimes being investigated because the information about the crimes was contained in an affidavit attached to the warrant); United States v. Ellis, 971 F.2d 701, 704 (11th Cir. 1992) (implying that the incorrect name on a warrant could have been cured if the correct name had appeared in the affidavit or if the officers had previously observed the premises). Additionally, the detailed list of items to be searched for, including the precisely-described suspect device, along with items showing evidence of child pornography, provided additional assurances that the searchers would understand where they were allowed to search. See Rousseau, 628 F. App'x at 1025-26.

Finally, the fact that Agent Thomas was present during the execution of the warrant further lessened the risk that the agents would conduct a broad, general search. See Burke, 784 F.2d at 1092-93 (holding that errors in the description of the place to be searched in the warrant were cured by the fact that the agent knew precisely which premises were to be searched and pointed out the correct apartment to the executing officer so that there was no possibility the wrong premises would be searched). Under the circumstances, there was little risk of the type of wide-ranging exploratory search that the Fourth Amendment guards against. Nor was there a risk that non-targets would mistakenly be subject to search, given the non-intrusive investigative techniques being employed by the agents. See United States v. Johnson, 290 F. App'x 214, 221-22 (11th Cir. 2008).

Defendant next argues that even if the warrant was sufficient to authorize the sniffer search of the entire building, the agents exceeded the warrant's authority by entering Defendant's office. According to Defendant, the agents should have applied for a second warrant before searching his office. (Doc. 42 at 4). Defendant argues that "[a]t any point during the 10 days that the agents conducted their investigation to narrow the search, including the moment that they were standing outside of [Defendant's] office door, they could have easily obtained a

subsequent warrant to further narrow the search but they failed to do so.” (Doc. 39 at 6).

In support of this argument, Defendant relies upon a recent U.S. Supreme Court case, Florida v. Jardines, ___ U.S. ___ 133 S. Ct. 1409 (2013), that dealt with the use of drug sniffing dogs without a warrant. In Jardines, the Supreme Court held that the use of trained police dogs to investigate a home and its surrounding area amounts to a search under the Fourth Amendment, requiring a warrant. Id. at 1417. Nothing in Jardines, however, suggests that if law enforcement obtains a warrant to use a drug dog (or other “sniffing” tool) in the first instance, that they will be required to obtain a second warrant if the dog (or other “sniffing” tool) locates the target of the search. In the present case, unlike Jardines, the agents properly obtained a warrant prior to embarking on their “sniffing” activities. Having located the suspect device, and armed with a warrant specifically authorizing them to seize the device, the agents acted appropriately and with authority.

2. The things to be seized

The warrant provides as follows with respect to the property or things to be seized:

1. A wireless device containing the Medial [sic] Access Control (MAC) address “68:a3:c4:e2:6a:7e”;
2. Electronic data processing and storage devices;

3. Computers and computer systems, internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and disks, tape drives and tapes, optical storage devices, CD's, DVD's or other memory storage devices;
4. Peripheral input/output devices such as keyboards, printers, video display monitors, optical readers, and related communications devices such as modems;
5. Backup media;
6. System documentation;
7. Software and instruction manuals;
8. Image files, either printed or electronic, that constitute evidence of a violation of O.C.G.A. 16-12-100(b)(8), possession of child pornography;
9. Movie files, that constitute evidence of a violation of O.C.G.A. 16-12-100(b)(8), possession of child pornography;
10. All of the above records whether stored on paper, on magnetic media such as tape, cassette, disk, CD, DVD or on memory storage devices such as optical disks, programmable instruments such as telephones, "electronic calendar/address books" calculators, wristwatches, personal communication service (PCS) devices, or any other storage media together with indicia of use, ownership, possession or control of such records;
11. Books, magazines, articles, newspapers, photographs, negatives, slides, movies, albums, drawings, audiotapes, personal letters, diaries, paintings, photographic equipment, etc., that would tend to show contact with minors or would constitute evidence of a violation of O.C.G.A. 16-12-100(b)(8) possession of child pornography;

12. Cellular telephones which can now be used to take, and transmit image files and movie files as well as text messaging, that constitute evidence of a violation of O.C.G.A. 16-12-100(b)(5), possession of child pornography.
13. Digital communications, printed or electronic, such as text messages, instant messages, e-mails, chats, that constitute evidence of a violation of O.C.G.A. 16-12-100(b)(8), possession of child pornography.

Which is (name the law being violated) in violation of:

O.C.G.A. 16-12-100: Sexual Exploitation of Children

O.C.G.A. 16-12-100 (b)(8): Possession of Child Pornography

O.C.G.A. 16-1-100 (b)(5): Distribution of Child Pornography

(Doc. 33-1 at 1-2).

The Eleventh Circuit instructs that the particularity requirement with respect to items to be seized “be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of property will be acceptable if it is as specific as the circumstances and nature of activity under investigation permit.” United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir. 1982) (citations omitted). Defendant argues that the things to be seized were not described with sufficient particularity because, other than the one mobile device identified by MAC address, the categories of items—such as backup media,

software, images, records, telephones, etc.—were overly broad and were not limited in any way. (Doc. 39 at 2). I disagree.

By explicitly limiting the scope of what may be searched and seized to evidence of the crimes under investigation (Georgia statutes concerning child pornography and sexual exploitation of children), the warrant was sufficiently particular to enable the searcher to reasonably ascertain and identify the property authorized to be seized. See Signature Pharmacy, Inc. v. Wright, 438 F. App'x 741, 745-46 (11th Cir. 2011) (per curiam) (unpublished) (holding that the items to be seized were described with sufficient particularity where the items were limited by the specific crimes under investigation and stating “[b]ecause the descriptions in the warrants refer to items that are evidence of a violation of certain statutes relating to the sale of controlled substances, the items were described with sufficient particularity to allow Wright, a seasoned law enforcement officer, to identify the things to be seized”); United States v. Harvey, No. 1:15-cr-00053-TWT-RGV, 2015 WL 9685908, at *13 (N.D. Ga. Nov. 30, 2015), adopted by 2016 WL 109984, at *1 (N.D. Ga. Jan. 8, 2016) (concluding that a search warrant for a cell phone was sufficiently particularized where the property to be seized was limited to evidence of the crimes being investigated). The universe of property that could be seized pursuant to the warrant at issue in this case was limited to

evidence of illegal activities concerning sexual exploitation of minors and child pornography. The warrant, therefore, did not permit a general exploratory search. See United States v. Brooks, No. 3:13-cr-58-J-34JRK, 2014 WL 292194, at *11 (M.D. Fla. Jan. 27, 2014) (concluding that because the scope of the warrant was restricted to evidence of child pornography-related crimes, it did not permit a free-ranging search).

B. Good Faith Reliance on the Warrant

The Government next argues, in the alternative, that even if the warrant was invalid due to lack of particularity, the good faith exception to the exclusionary rule would validate this warrant. In United States v. Leon, the Supreme Court held that the Fourth Amendment exclusionary rule should not be applied so as to exclude evidence obtained by officers acting in reasonable reliance on an invalid search warrant issued by a detached and neutral magistrate. 468 U.S. 897, 922 (1984). This is known as the good-faith exception to the exclusionary rule and applies when law enforcement officers executing the warrant act “in the objectively reasonable belief that their conduct does not violate the Fourth Amendment.” Id. at 918. The Eleventh Circuit has recognized only four circumstances that prevent the use of the good-faith exception:

- (1) where the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would

have known was false except for his reckless disregard of the truth; (2) where the issuing magistrate wholly abandoned his judicial role . . . ; (3) where the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where, depending upon the circumstances of the particular case, a warrant is so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.

United States v. Martin, 297 F.3d 1308, 1313 (11th Cir. 2002) (internal citations and quotation marks omitted). Here, Defendant argues that the fourth circumstance applies, i.e., that the warrant was so facially deficient that no officer could reasonably presume it to be valid. (Doc. 42 at 7). This argument lacks merit.

In this case, it is evident that the good faith exception under Leon applies. None of the circumstances that might make an officer's reliance unreasonable are presented here. There is no evidence that the affidavit in this case was recklessly or deliberately false. There is no evidence that the affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," or that the warrant was "so facially deficient that an officer could not reasonably presume it to be valid." Finally there is certainly no evidence that the issuing judge wholly abandoned his or her judicial role in issuing the warrant.

See Leon, 468 U.S. at 923; see also United States v. Taxacher, 902 F.2d 867, 871 (11th Cir. 1990).

As the Government points out in its brief, the search warrant, when taken together with the detailed supporting affidavit, particularly described the place to be searched (the Rollins Building), the manner that the search was to be conducted (using the non-invasive sniffer), and the purpose of the search (to locate the very specifically-described suspect device and other evidence of child pornography). As noted above, the warrant adequately described the items to be seized, beginning with the suspect device (described precisely by MAC address) and then moving on to items that could be related depending on where the suspect device was located—with the underpinning requirement that the electronic devices contained or could contain evidence of child pornography. See Rousseau, 628 F. App'x at 1026. Moreover, Agent Thomas testified that because the sniffer was new to her, she consulted with counsel from Homeland Security and Emory University, sent them the search warrant to review, and relied on their assessment that the warrant was legally sufficient. Given the level of detail in the affidavit, the precision of the police work involved, and the caution with which Agent Thomas proceeded, it cannot be said that an executing officer could not reasonably have presumed the

warrant to be valid. Thus, even if the warrant were invalid, the motion to suppress should still be denied based on the good faith exception to the exclusionary rule.

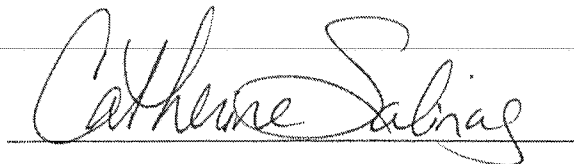
III. CONCLUSION

IT IS HEREBY ORDERED that Defendant's Motion for Bill of Particulars and for Further Rule 16 Discovery and Brady Information (Doc. 27) is **DENIED AS MOOT**.

IT IS RECOMMENDED that Defendant's Motion to Suppress and Supplemental Motion to Suppress (Docs. 26, 33) be **DENIED**.

I have now addressed all referred pretrial matters and have not been advised of any impediments to the scheduling of a trial. Accordingly, this case is **CERTIFIED READY FOR TRIAL**.

IT IS SO ORDERED, REPORTED, AND RECOMMENDED this 25th day of May, 2016.

A handwritten signature in cursive script, reading "Catherine Salinas", written over a horizontal line.

CATHERINE M. SALINAS
United States Magistrate Judge